PKIX Working Group S. Chokhani (CygnaCom Solutions, Inc.)
Internet Draft W. Ford (VeriSign, Inc.)

Expires in six months from April 25, 1998

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

<draft-ietf-pkix-ipki-part4-03.txt>

Status of this Memo

Abstract

This document presents a framework to assist the writers of certificate policies or certification practice statements for certification authorities and public key infrastructures. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy definition or a certification practice statement. This document is being submitted to the RFC Editor with a request for publication as an Informational RFC.

1. INTRODUCTION

1.1 BACKGROUND

A public-key certificate (hereinafter "certificate") binds a public-key value to a set of information that identifies the

entity (such as person, organization, account, or site) associated with use of the corresponding private key (this entity is known as the "subject" of the certificate). A certificate is used by a "certificate user" or "relying party" that needs to use, and rely upon the accuracy of, the public key distributed via that certificate (a certificate user is typically an entity that is verifying a digital signature from the certificate's subject or an entity sending encrypted data to the subject). The degree to which a certificate user can trust the binding embodied in a certificate depends on several factors. These factors include the practices followed by the certification authority (CA) in authenticating the subject; the CA's operating policy, procedures, and security controls; the subject's obligations (for example, in protecting the private key); and the stated undertakings and legal obligations of the CA (for example, warranties and limitations on liability).

A Version 3 X.509 certificate may contain a field declaring that one or more specific certificate policies applies to that certificate [ISO1]. According to X.509, a certificate policy is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." A certificate policy may be used by a certificate user to help in deciding whether a certificate, and the binding therein, is sufficiently trustworthy for a particular application. The certificate policy concept is an outgrowth of the policy statement concept developed for Internet Privacy Enhanced Mail [PEM1] and expanded upon in [BAU1].

A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a certification practice statement (CPS) published by or referenced by the CA. According to the American Bar Association Digital Signature Guidelines (hereinafter "ABA Guidelines"), "a CPS is a statement of the practices which a certification authority employs in issuing certificates." [ABA1]

1.2 PURPOSE

The purpose of this document is to establish a clear relationship between certificate policies and CPSs, and to present a framework to assist the writers of certificate policies or CPSs with their tasks. In particular, the framework identifies the elements that may need to be considered in formulating a certificate policy or a CPS. The purpose is not to define particular certificate policies or CPSs, per se.

1.3 SCOPE

The scope of this document is limited to discussion of the contents of a certificate policy (as defined in X.509) or CPS (as defined in the ABA Guidelines). In particular, this document describes the types of information that should be considered for inclusion in a certificate policy definition or a CPS. While the framework as presented generally assumes use of the X.509 version 3 certificate format, it is not intended that the material be restricted to use of that certificate format. Rather, it is intended that this framework be adaptable to other certificate formats that may come into use.

The scope does not extend to defining security policies generally (such as organization security policy, system security policy, or data labeling policy) beyond the policy elements that are considered of particular relevance to certificate policies or CPSs.

This document does not define a specific certificate policy or CPS.

It is assumed that the reader is familiar with the general concepts of digital signatures, certificates, and public-key infrastructure, as used in X.509 and the ABA Guidelines.

2. DEFINITIONS

This document makes use of the following defined terms:

Activation data - Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

CA-certificate - A certificate for one CA's public key issued by another CA.

Certificate policy - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path - An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) - A statement of the practices which a certification authority employs in issuing certificates.

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Policy qualifier - Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Registration authority (RA) - An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is used elsewhere for the same concept.]

Relying party - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Set of provisions - A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.

Subject certification authority (subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

3. CONCEPTS

This section explains the concepts of certificate policy and CPS, and describes their relationship. Other related concepts are also described. Some of the material covered in this section and in some other sections is specific to certificate policies extensions as defined X.509 version 3. Except for those sections, this framework is intended to be adaptable to other certificate formats that may come into use.

3.1 CERTIFICATE POLICY

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a relying party) that a particular public key is bound to a particular

entity (the certificate subject). However, the extent to which the certificate user should rely on that statement by the CA needs to be assessed by the certificate user. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

The X.509 standard defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements"[ISO1]. An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

A certificate policy, which needs to be recognized by both the issuer and user of a certificate, is represented in a certificate by a unique, registered Object Identifier. The registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the Object Identifier also publishes a textual specification of the certificate policy, for examination by certificate users. Any one certificate will typically declare a single certificate policy or, possibly, be issued consistent with a small number of different policies.

Certificate policies also constitute a basis for accreditation of CAs. Each CA is accredited against one or more certificate policies which it is recognized as implementing. When one CA issues a CA-certificate for another CA, the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon accreditation with respect to the certificate policies involved). The assessed set of certificate policies is then indicated by the issuing CA in the CA-certificate. The X.509 certification path processing logic employs these certificate policy indications in its well-defined trust model.

3.2 CERTIFICATE POLICY EXAMPLES

For example purposes, suppose that IATA undertakes to define some certificate policies for use throughout the airline industry, in a public-key infrastructure operated by IATA in combination with public-key infrastructures operated by individual airlines. Two certificate policies are defined - the IATA General-Purpose policy, and the IATA Commercial-Grade policy.

The IATA General-Purpose policy is intended for use by industry personnel for protecting routine information (e.g., casual electronic mail) and for authenticating connections from World

Wide Web browsers to servers for general information retrieval purposes. The key pairs may be generated, stored, and managed using low-cost, software-based systems, such as commercial browsers. Under this policy, a certificate may be automatically issued to anybody listed as an employee in the corporate directory of IATA or any member airline who submits a signed certificate request form to a network administrator in his or her organization.

The IATA Commercial-Grade policy is used to protect financial transactions or binding contractual exchanges between airlines. Under this policy, IATA requires that certified key pairs be generated and stored in approved cryptographic hardware tokens. Certificates and tokens are provided to airline employees with disbursement authority. These authorized individuals are required to present themselves to the corporate security office, show a valid identification badge, and sign an undertaking to protect the token and use it only for authorized purposes, before a token and a certificate are issued.

3.3 X.509 CERTIFICATE FIELDS

The following extension fields in an X.509 certificate are used to support certificate policies:

* Certificate Policies extension;
* Policy Mappings extension; and
* Policy Constraints extension.

3.3.1 Certificate Policies Extension

The Certificate Policies extension has two variants - one with the field flagged non-critical and one with the field flagged critical. The purpose of the field is different in the two cases.

A non-critical Certificate Policies field lists certificate policies that the certification authority declares are applicable. However, use of the certificate is not restricted to the purposes indicated by the applicable policies. Using the example of the IATA General- Purpose and Commercial-Grade policies defined in Section 3.2, the certificates issued to regular airline employees will contain the object identifier for certificate policy for the General-Purpose policy. The certificates issued to the employees with disbursement authority will contain the object identifiers for both the General-Purpose policy and the Commercial-Grade policy. The Certificate Policies field may also optionally convey qualifier

values for each identified policy; use of qualifiers is discussed in Section 3.4.

The non-critical Certificate Policies field is designed to be used by applications as follows. Each application is pre-configured to know what policy it requires. Using the example in Section 3.2, electronic mail applications and Web servers will be configured to require the General-Purpose policy. However, an airline's financial applications will be configured to require the Commercial-Grade policy for validating financial transactions over a certain dollar value.

When processing a certification path, a certificate policy that is acceptable to the certificate-using application must be present in every certificate in the path, i.e., in CA-certificates as well as end entity certificates.

If the Certificate Policies field is flagged critical, it serves the same purpose as described above but also has an additional role. It indicates that the use of the certificate is restricted to one of the identified policies, i.e., the certification authority is declaring that the certificate must only be used in accordance with the provisions of one of the listed certificate policies. This field is intended to protect the certification authority against damage claims by a relying party who has used the certificate for an inappropriate purpose or in an inappropriate manner, as stipulated in the applicable certificate policy definition.

For example, the Internal Revenue Service might issue certificates to taxpayers for the purpose of protecting tax filings. The Internal Revenue Service understands and can accommodate the risks of accidentally issuing a bad certificate, e.g., to a wrongly- authenticated person. However, suppose someone used an Internal Revenue Service tax-filing certificate as the basis for encrypting multi-million-dollar-value proprietary secrets which subsequently fell into the wrong hands because of an error in issuing the Internal Revenue Service certificate. The Internal Revenue Service may want to protect itself against claims for damages in such circumstances. The critical-flagged Certificate Policies extension is intended to mitigate the risk to the certificate issuer in such situations.

3.3.2 Policy Mappings Extension

The Policy Mappings extension may only be used in CA-certificates. This field allows a certification authority to indicate that certain policies in its own domain can be considered equivalent to certain other policies in the subject certification authority's domain.

For example, suppose the ACE Corporation establishes an agreement with the ABC Corporation to cross-certify each others' public-key infrastructures for the purposes of mutually protecting electronic data interchange (EDI). Further, suppose that both companies have pre-existing financial transaction protection policies called ace-e- commerce and abc-e-commerce, respectively. One can see that simply generating cross certificates between the two domains will not provide the necessary interoperability, as the two companies' applications are configured with and employee certificates are populated with their respective certificate policies. One possible solution is to reconfigure all of the financial applications to require either policy and to reissue all the certificates with both policies. Another solution, which may be easier to administer, uses the Policy Mapping field. If this field is included in a cross-certificate for the ABC Corporation certification authority issued by the ACE Corporation certification authority, it can provide a statement that the ABC's financial transaction protection policy (i.e., abc-e-commerce) can be considered equivalent to that of the ACE Corporation (i.e., ace-e-commerce).

3.3.3 Policy Constraints Extension

The Policy Constraints extension supports two optional features. The first is the ability for a certification authority to require that explicit certificate policy indications be present in all subsequent certificates in a certification path. Certificates at the start of a certification path may be considered by a certificate user to be part of a trusted domain, i.e., certification authorities are trusted for all purposes so no particular certificate policy is needed in the Certificate Policies extension. Such certificates need not contain explicit indications of certificate policy. However, when a certification authority in the trusted domain certifies outside the domain, it can activate the requirement for explicit certificate policy in subsequent certificates in the certification path.

The other optional feature in the Policy Constraints field is

the ability for a certification authority to disable policy mapping by subsequent certification authorities in a certification path. It may be prudent to disable policy mapping when certifying outside the domain. This can assist in controlling risks due to transitive trust, e.g., a domain A trusts domain B, domain B trusts domain C, but domain A does not want to be forced to trust domain C.

3.4 POLICY QUALIFIERS

The Certificate Policies extension field has a provision for conveying, along with each certificate policy identifier, additional policy-dependent information in a qualifier field. The X.509 standard does not mandate the purpose for which this field is to be used, nor does it prescribe the syntax for this field. Policy qualifier types can be registered by any organization.

The following policy qualifier types are defined in PKIX Part I [PKI1]:

(a) The CPS Pointer qualifier contains a pointer to a Certification Practice Statement (CPS) published by the CA. The pointer is in the form of a uniform resource identifier (URI).

(b) The User Notice qualifier contains a text string that is to be displayed to a certificate user (including subscribers and relying parties) prior to the use of the certificate. The text string may be an IA5String or a BMPString - a subset of the ISO 100646-1 multiple octet coded character set. A CA may invoke a procedure that requires that the certficate user acknowledge that the applicable terms and conditions have been disclosed or accepted.

Policy qualifiers can be used to support the definition of generic, or parameterized, certificate policy definitions. Provided the base certificate policy definition so provides, policy qualifier types can be defined to convey, on a per-certificate basis, additional specific policy details that fill in the generic definition.

3.5 CERTIFICATION PRACTICE STATEMENT

The term certification practice statement (CPS) is defined by the ABA Guidelines as: "A statement of the practices which a certification authority employs in issuing certificates." [ABA1] In the 1995 draft of the ABA guidelines, the ABA expands this definition with the following comments:

A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate, or it may be a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber. A certification practice statement may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration.

Certain forms for legally implementing certification practice statements lend themselves to particular relationships. For example, when the legal relationship between a certification authority and subscriber is consensual, a contract would ordinarily be the means of giving effect to a certification practice statement. The certification authority's duties to a relying person are generally based on the certification authority's representations, which may include a certification practice statement.

Whether a certification practice statement is binding on a relying person depends on whether the relying person has knowledge or notice of the certification practice statement. A relying person has knowledge or at least notice of the contents of the certificate used by the relying person to verify a digital signature, including documents incorporated into the certificate by reference. It is therefore advisable to incorporate a certification practice statement into a certificate by reference.

As much as possible, a certification practice statement should indicate any of the widely recognized standards to which the certification authority's practices conform. Reference to widely recognized standards may indicate concisely the suitability of the certification authority's practices for another person's purposes, as well as the potential technological compatibility of the certificates issued by the certification authority with repositories and other systems.

3.6 RELATIONSHIP BETWEEN CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

The concepts of certificate policy and CPS come from different sources and were developed for different reasons. However, their interrelationship is important.

A certification practice statement is a detailed statement by a

certification authority as to its practices, that potentially needs to be understood and consulted by subscribers and certificate users (relying parties). Although the level of detail may vary among CPSs, they will generally be more detailed than certificate policy definitions. Indeed, CPSs may be quite comprehensive, robust documents providing a description of the precise service offerings, detailed procedures of the life- cycle management of certificates, and more - a level of detail which weds the CPS to a particular (proprietary) implementation of a service offering.

Although such detail may be indispensable to adequately disclose, and to make a full assessment of trustworthiness in the absence of accreditation or other recognized quality metrics, a detailed CPS does not form a suitable basis for interoperability between CAs operated by different organizations. Rather, certificate policies best serve as the vehicle on which to base common interoperability standards and common assurance criteria on an industry-wide (or possibly more global) basis. A CA with a single CPS may support multiple certificate policies (used for different application purposes and/or by different certificate user communities). Also, multiple different CAs, with non-identical certification practice statements, may support the same certificate policy.

For example, the Federal Government might define a government-wide certificate policy for handling confidential human resources information. The certificate policy definition will be a broad statement of the general characteristics of that certificate policy, and an indication of the types of applications for which it is suitable for use. Different departments or agencies that operate certification authorities with different certification practice statements might support this certificate policy. At the same time, such certification authorities may support other certificate policies.

The main difference between certificate policy and CPS can therefore be summarized as follows:

(a) Most organizations that operate public or inter-organizational certification authorities will document their own practices in CPSs or similar statements. The CPS is one of the organization's means of protecting itself and positioning its business relationships with subscribers and other entities.

(b) There is strong incentive, on the other hand, for a certificate policy to apply more broadly than to just a single organization. If a particular certificate policy is widely recognized and imitated, it has great potential as the basis of

automated certificate acceptance in many systems, including unmanned systems and systems that are manned by people not independently empowered to determine the acceptability of different presented certificates.

In addition to populating the certificate policies field with the certificate policy identifier, a certification authority may include, in certificates it issues, a reference to its certification practice statement. A standard way to do this, using a certificate policy qualifier, is described in Section 3.4.

3.7 SET OF PROVISIONS

A set of provisions is a collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.

A certificate policy can be expressed as a single set of provisions.

A CPS can be expressed as a single set of provisions with each component addressing the requirements of one or more certificate policies, or, alternatively, as an organized collection of sets of provisions. For example, a CPS could be expressed as a combination of the following:

(a) a list of certificate policies supported by the CPS;

(b) for each certificate policy in (a), a set of provisions which contains statements that refine that certificate policy by filling in details not stipulated in that policy or expressly left to the discretion of the CPS by that certificate policy; such statements serve to state how this particular CPS implements the requirements of the particular certificate policy;

(c) a set of provisions that contains statements regarding the certification practices on the CA, regardless of certificate policy.

The statements provided in (b) and (c) may augment or refine the stipulations of the applicable certificate policy definition, but must not conflict with any of the stipulations of such certificate policy definition.

This framework outlines the contents of a set of provisions, in terms of eight primary components, as follows:

* Introduction;

* General Provisions;

* Identification and Authentication;

* Operational Requirements;

* Physical, Procedural, and Personnel Security Controls;

* Technical Security Controls;

* Certificate and CRL Profile; and

* Specification Administration.

Components can be further divided into subcomponents, and a subcomponent may comprise multiple elements. Section 4 provides a more detailed description of the contents of the above components, and their subcomponents.

4. CONTENTS OF A SET OF PROVISIONS

This section expands upon the contents of a set of provisions, as introduced in Section 3.7. The topics identified in this section are, consequently, candidate topics for inclusion in a certificate policy definition or CPS.

While many topics are identified, it is not necessary for a certificate policy or a CPS to include a concrete statement for every such topic. Rather, a particular certificate policy or CPS may state "no stipulation" for a component, subcomponent, or element on which the particular certificate policy or CPS imposes no requirements. In this sense, the list of topics can be considered a checklist of topics for consideration by the certificate policy or CPS writer. It is recommended that each and every component and subcomponent be included in a certificate policy or CPS, even if there is "no stipulation"; this will indicate to the reader that a conscious decision was made to include or exclude that topic. This protects against inadvertent omission of a topic, while facilitating comparison of different certificate policies or CPSs, e.g., when making policy mapping decisions.

In a certificate policy definition, it is possible to leave certain components, subcomponents, and/or elements unspecified, and to stipulate that the required information will be indicated in a policy qualifier. Such certificate policy definitions can be considered

parameterized definitions. The set of provisions should reference or define the required policy qualifier types and should specify any applicable default values.

4.1 INTRODUCTION

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the specification is targeted.

This component has the following subcomponents:

* Overview;

* Identification;

* Community and Applicability; and

* Contact Details.

4.1.1 Overview

This subcomponent provides a general introduction to the specification.

4.1.2 Identification

This subcomponent provides any applicable names or other identifiers, including ASN.1 object identifiers, for the set of provisions.

4.1.3 Community and Applicability

This subcomponent describes the types of entities that issue certificates or that are certified as subject CAs (2, 3), the types of entities that perform RA functions (4), and the types of entities that are certified as subject end entities or subscribers. (5, 6)

This subcomponent also contains:

* A list of applications for which the issued certificates are suitable. (Examples of application in this case are: electronic mail, retail transactions, contracts, travel order, etc.)

* A list of applications for which use of the issued certificates is restricted. (This list implicitly prohibits all other uses for the certificates.)

* A list of applications for which use of the issued certificates is prohibited.

4.1.4 Contact Details

This subcomponent includes the name and mailing address of the authority that is responsible for the registration, maintenance, and interpretation of this certificate policy or CPS. It also includes the name, electronic mail address, telephone number, and fax number of a contact person.

4.2 GENERAL PROVISIONS

This component specifies any applicable presumptions on a range of legal and general practices topics.

This component contains the following subcomponents:

* Obligations;

* Liability;

* Financial Responsibility;

* Interpretation and Enforcement;

* Fees;

* Publication and Repositories;

* Compliance Audit;

* Confidentiality; and

* Intellectual Property Rights.

Each subcomponent may need to separately state provisions applying to the entity types: CA, repository, RA, subscriber, and relying party. (Specific provisions regarding subscribers and relying parties are only applicable in the Liability and Obligations subcomponents.)

4.2.1 Obligations

This subcomponent contains, for each entity type, any applicable provisions regarding the entity's obligations to other entities. Such provisions may include:

* CA and/or RA obligations:
  * Notification of issuance of a certificate to the subscriber who is the subject of the certificate being issued;
  * Notification of issuance of a certificate to others than the subject of the certificate;
  * Notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended; and
  * Notification of revocation or suspension of a certificate to others than the subject whose certificate is being revoked or suspended.

* Subscriber obligations:

  * Accuracy of representations in certificate application;
  * Protection of the entity's private key;
  * Restrictions on private key and certificate use; and
  * Notification upon private key compromise.

* Relying party obligations:

  * Purposes for which certificate is used;
  * Digital signature verification responsibilities;
  * Revocation and suspension checking responsibilities; and
  * Acknowledgment of applicable liability caps and warranties.

* Repository obligations

  * Timely publication of certificates and revocation information

4.2.2 Liability

This subcomponent contains, for each entity type, any applicable provisions regarding apportionment of liability, such as:

* Warranties and limitations on warranties;

* Kinds of damages covered (e.g., indirect, special, consequential, incidental, punitive, liquidated damages, negligence and fraud) and disclaimers;

* Loss limitations (caps) per certificate or per transaction; and

* Other exclusions (e.g., Acts of God, other party responsibilities).

4.2.3 Financial Responsibility

This subcomponent contains, for CAs, repository, and RAs, any applicable provisions regarding financial responsibilities, such as:

* Indemnification of CA and/or RA by relying parties;

* Fiduciary relationships (or lack thereof) between the various entities; and

* Administrative processes (e.g., accounting, audit).

4.2.4 Interpretation and Enforcement

This subcomponent contains any applicable provisions regarding interpretation and enforcement of the certificate policy or CPS, addressing such topics as:

* Governing law;

* Severability of provisions, survival, merger, and notice; and

* Dispute resolution procedures.

4.2.5 Fees

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs, such as:

* Certificate issuance or renewal fees;

* Certificate access fee;

* Revocation or status information access fee;

* Fees for other services such as policy information; and

* Refund policy.

4.2.6 Publication and Repositories

This subcomponent contains any applicable provisions regarding:

* A CA's obligations to publish information regarding its practices, its certificates, and the current status of such certificates;

* Frequency of publication;

* Access control on published information objects including certificate policy definitions, CPS, certificates, certificate status, and CRLs; and

* Requirements pertaining to the use of repositories operated by CAs or by other independent parties.

4.2.7 Compliance Audit

This subcomponent addresses the following:

* Frequency of compliance audit for each entity;

* Identity/qualifictions of the auditor;

* Auditor's relationship to the entity being audited; (30)

* List of topics covered under the compliance audit; (31)

* Actions taken as a result of a deficiency found during compliance audit; (32)

* Compliance audit results: who they are shared with (e.g.,

subject CA, RA, and/or end entities), who provides them (e.g., entity being audited or auditor), how they are communicated.

4.2.8 Confidentiality Policy

This subcomponent addresses the following:

* Types of information that must be kept confidential by CA or RA;

* Types of information that are not considered confidential;

* Who is entitled to be informed of reasons for revocation and suspension of certificates;

* Policy on release of information to law enforcement officials;

* Information that can be revealed as part of civil discovery;

* Conditions upon which CA or RA may disclose upon owner's request; and

* Any other circumstances under which confidential information may be disclosed.

4.2.9 Intellectual Property Rights

This subcomponent addresses ownership rights of certificates, practice/policy specifications, names, and keys.

4.3 IDENTIFICATION AND AUTHENTICATION

This component describes the procedures used to authenticate a certificate applicant to a CA or RA prior to certificate issuance. It also describes how parties requesting rekey or revocation are authenticated. This component also addresses naming practices, including name ownership recognition and name dispute resolution.

This component has the following subcomponents:

* Initial Registration;

* Routine Rekey;

* Rekey After Revocation; and

* Revocation Request.

4.3.1 Initial Registration

This subcomponent includes the following elements regarding identification and authentication procedures during entity registration or certificate issuance:

* Types of names assigned to the subject (7);

* Whether names have to be meaningful or not (8);

* Rules for interpreting various name forms;

* Whether names have to be unique;

* How name claim disputes are resolved;

* Recognition, authentication, and role of trademarks;

* If and how the subject must prove possession of the companion private key for the public key being registered (9);

* Authentication requirements for organizational identity of subject (CA, RA, or end entity) (10);

* Authentication requirements for a person acting on behalf of a subject (CA, RA, or end entity) (11), including:

  * Number of pieces of identification required;
  * How a CA or RA validates the pieces of identification provided;
  * If the individual must present personally to the authenticating CA or RA;
  * How an individual as an organizational person is authenticated (12).

4.3.2 Routine Rekey

This subcomponent describes the identification and authentication procedures for routine rekey for each subject type (CA, RA, and end entity). (13)

4.3.3 Rekey After Revocation -- No Key Compromise

This subcomponent describes the identification and authentication procedures for rekey for each subject type (CA, RA, and end entity) after the subject certificate has been revoked. (14)

4.3.4 Revocation Request

This subcomponent describes the identification and authentication procedures for a revocation request by each subject type (CA, RA, and end entity). (16)

4.4 OPERATIONAL REQUIREMENTS

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, or end entities with respect to various operational activities.

This component consists of the following subcomponents:

* Certificate Application;

* Certificate Issuance;

* Certificate Acceptance;

* Certificate Suspension and Revocation;

* Security Audit Procedures;

* Records Archival;

* Key Changeover;

* Compromise and Disaster Recovery; and

* CA Termination.

Within each subcomponent, separate consideration may need to be given to issuing CA, repository, subject CAs, RAs, and end entities.

4.4.1 Certificate Application

This subcomponent is used to state requirements regarding subject enrollment and request for certificate issuance.

4.4.2 Certificate Issuance

This subcomponent is used to state requirements regarding issuance of a certificate and notification to the applicant of such issuance.

4.4.3 Certificate Acceptance

This subcomponent is used to state requirements regarding acceptance of an issued certificate and for consequent publication of certificates.

4.4.4 Certificate Suspension and Revocation

This subcomponent addresses the following:

* Circumstances under which a certificate may be revoked;

* Who can request the revocation of the entity certificate;

* Procedures used for certificate revocation request;

* Revocation request grace period available to the subject;

* Circumstances under which a certificate may be suspended;

* Who can request the suspension of a certificate;

* Procedures to request certificate suspension;

* How long the suspension may last;

* If a CRL mechanism is used, the issuance frequency;

* Requirements on relying parties to check CRLs;

* On-line revocation/status checking availability;

* Requirements on relying parties to perform on-line revocation/status checks;

* Other forms of revocation advertisements available; and

* Requirements on relying parties to check other forms of revocation advertisements.

* Any variations on the above stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).

4.4.5 Security Audit Procedures

This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining a secure environment. Elements include the following:

* Types of events recorded; (28)

* Frequency with which audit logs are processed or audited;

* Period for which audit logs are kept;

* Protection of audit logs:

  - Who can view audit logs;
  - Protection against modification of audit log; and
  - Protection against deletion of audit log.

* Audit log back up procedures;

* Whether the audit log accumulation system is internal or external to the entity;

* Whether the subject who caused an audit event to occur is notified of the audit action; and

* Vulnerability assessments.

4.4.6 Records Archival

This subcomponent is used to describe general records archival (or records retention) policies, including the following:

* Types of events recorded; (29)

* Retention period for archive;

* Protection of archive:

  - Who can view the archive;
  - Protection against modification of archive; and

- Protection against deletion of archive.

* Archive backup procedures;

* Requirements for time-stamping of records;

* Whether the archive collection system is internal or external; and

* Procedures to obtain and verify archive information.

4.4.7 Key Changeover

This subcomponent describes the procedures to provide a new public key to a CA's users.

4.4.8 Compromise and Disaster Recovery

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following circumstances may need to be addressed separately:

* The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is reestablished, which certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the subjects are recertified.

* The recovery procedures used if the entity public key is revoked. These procedures describe how a secure environment is reestablished, how the new entity public key is provided to the users, and how the subjects are recertified.

* The recovery procedures used if the entity key is compromised. These procedures describe how a secure environment is reestablished, how the new entity public key is provided to the users, and how the subjects are recertified.

* The CA's procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is reestablished either at the original site or a remote hot-site. For example, procedures to protect against theft of sensitive materials from an earthquake-damaged site.

4.4.9 CA Termination

This subcomponent describes requirements relating to procedures for termination and for termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records.

4.5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

This component can also be used to define non-technical security controls on repository, subject CAs, RAs, and end entities. The non technical security controls for the subject CAs, RAs, and end entities could be the same, similar, or very different.

These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations resulting, for example, in the creation of certificates or CRLs with erroneous information or the compromise of the CA private key.

This component consists of three subcomponents:

* Physical Security Controls;

* Procedural Controls; and

* Personnel Security Controls.

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, that is, issuing CA, repository, subject CAs, RAs, and end entities.

4.5.1 Physical Security Controls

In this subcomponent, the physical controls on the facility housing the entity systems are described.(21) Topics addressed may include:

* Site location and construction;

* Physical access;

* Power and air conditioning;

* Water exposures;

* Fire prevention and protection;

* Media storage;

* Waste disposal; and

* Off-site backup.

4.5.2 Procedural Controls

In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22)

For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule). Identification and authentication requirements for each role may also be defined.

4.5.3 Personnel Security Controls

This subcomponent addresses the following:

* Background checks and clearance procedures required for the personnel filling the trusted roles; (23)

* Background checks and clearance procedures requirements for other personnel, including janitorial staff; (24)

* Training requirements and training procedures for each role;

* Any retraining period and retraining procedures for each role;

* Frequency and sequence for job rotation among various roles;

* Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems; (25)

* Controls on contracting personnel, including:

- Bonding requirements on contract personnel;
- Contractual requirements including indemnification for damages due to the actions of the contractor personnel;
- Audit and monitoring of contractor personnel; and
- Other controls on contracting personnel.

* Documentation to be supplied to personnel.

4.6 TECHNICAL SECURITY CONTROLS

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on repositories, subject CAs and end entities to protect their cryptographic keys and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, audit, and archival. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs, and end entities.

This component has the following subcomponents:

* Key Pair Generation and Installation;

* Private Key Protection;

* Other Aspects of Key Pair Management;

* Activation Data;

* Computer Security Controls;

* Life-Cycle Security Controls;

* Network Security Controls; and

* Cryptographic Module Engineering Controls.

4.6.1 Key Pair Generation and Installation

Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs, and subject end entities. For each of these types of entities, the following questions potentially need to be answered:

1. Who generates the entity public, private key pair?

2. How is the private key provided securely to the entity?

3. How is the entity's public key provided securely to the certificate issuer?

4. If the entity is a CA (issuing or subject) how is the entity's public key provided securely to the users?

5. What are the key sizes?

6. Who generates the public key parameters?

7. Is the quality of the parameters checked during key generation?

8. Is the key generation performed in hardware or software?

9. For what purposes may the key be used, or for what purposes should usage of the key be restricted (for X.509 certificates, these purposes should map to the key usage flags in the Version 3, X.509 certificates)?

4.6.2 Private Key Protection

Requirements for private key protection need to be considered for the issuing CA, repositories, subject CAs, RAs, and subject end entities. For each of these types of entity, the following questions potentially need to be answered:

1. What standards, if any, are required for the module used to generate the keys? For example, are the keys certified by the infrastructure required to be generated using modules complaint with the US FIPS 140-1? If so, what is the required FIPS 140-1 level of the module?

2. Is the private key under n out of m multi-person control?(18) If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?

3. Is the private key escrowed? (19) If so, who is the escrow agent, what form is the key escrowed in (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?

4. Is the private key backed up? If so, who is the backup agent, what form is the key backed up in (examples include plaintext, encrypted, split key), and what are the security controls on the backup system?

5. Is the private key archived? If so, who is the archival agent, what form is the key archived in (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?

6. Who enters the private key in the cryptographic module? In what form (i.e., plaintext, encrypted, or split key)? How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?

7. Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?

8. Who can deactivate the private key and how? Example of how might include, logout, power off, remove token/key, automatic, or time expiration.

9. Who can destroy the private key and how? Examples of how might include token surrender, token destruction, or key overwrite.

4.6.3 Other Aspects of Key Pair Management

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, and subject end entities. For each of these types of entity, the following questions potentially need to be answered:

1. Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system? The archival system should provide integrity controls other than digital signatures since: the archival period may be greater than the cryptanalysis period for the key and the archive requires tamper protection, which is not

provided by digital signatures.

2. What are the usage periods, or active lifetimes, for the public and the private key respectively?

4.6.4 Activation Data

Activation data refers to data values other than keys that are required to operate cryptographic modules and that need to be protected. (20) Protection of activation data potentially needs to be considered for the issuing CA, subject CAs, RAs, and end entities. Such consideration potentially needs to address the entire life-cycle of the activation data from generation through archival and destruction. For each of the entity types (issuing CA, repository, subject CA, RA, and end entity) all of the questions listed in 4.6.1 through 4.6.3 potentially need to be answered with respect to activation data rather than with respect to keys.

4.6.5 Computer Security Controls

This subcomponent is used to describe computer security controls such as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object reuse, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), or the Common Criteria. This subcomponent can also address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity undertaken.

4.6.6 Life Cycle Security Controls

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g., defensive programming) and development

facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life- cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).

4.6.7 Network Security Controls

This subcomponent addresses network security related controls, including firewalls.

4.6.8 Cryptographic Module Engineering Controls (26)

This subcomponent addresses the following aspects of a cryptographic module: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests. Requirements may be expressed through reference to a standard such as U.S. FIPS 140-1. (27)

4.7 CERTIFICATE AND CRL PROFILES

This component is used to specify the certificate format and, if CRLs are used, the CRL format. Assuming use of the X.509 certificate and CRL formats, this includes information on profiles, versions, and extensions used.

This component has two subcomponents:

* Certificate Profile; and

* CRL Profile.

4.7.1 Certificate Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the PKIX Part I profile):

* Version number(s) supported;

* Certificate extensions populated and their criticality;

* Cryptographic algorithm object identifiers;

* Name forms used for the CA, RA, and end entity names;

* Name constraints used and the name forms used in the name constraints;

* Applicable certificate policy Object Identifier(s);

* Usage of the policy constraints extension;

* Policy qualifiers syntax and semantics; and

* Processing semantics for the critical certificate policy extension.

4.7.2 CRL Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the PKIX Part I profile):

* Version numbers supported for CRLs; and

* CRL and CRL entry extensions populated and their criticality.

4.8 SPECIFICATION ADMINISTRATION

This component is used to specify how this particular certificate policy definition or CPS will be maintained.

It contains the following subcomponents:

* Specification Change Procedures;

* Publication and Notification Procedures; and

* CPS Approval Procedures.

4.8.1 Specification Change Procedures

It will occasionally be necessary to change certificate policies and Certification Practice Statements. Some of these changes will not materially reduce the assurance that a certificate policy or its implementation provides, and will be judged by the policy administrator as not changing the acceptability of certificates asserting the policy for the purposes for which they have been used. Such changes to certificate policies and Certification Practice Statements need not require a change in the certificate policy Object Identifier or the CPS pointer (URL). Other changes to a specification will change the acceptability of certificates for specific purposes, and these changes will require changes to the certificate policy Object Identifier or CPS pointer (URL).

This subcomponent contains the following information:

* A list of specification components, subcomponents, and/or elements thereof that can be changed without notification and without changes to the certificate policy Object Identifier or CPS pointer (URL).

* A list of specification components, subcomponents, and/or elements thereof that may change following a notification period without changing the certificate policy Object Identifier or CPS pointer (URL). The procedures to be used to notify interested parties (relying parties, certification authorities, etc.) of the certificate policy or CPS changes are described. The description of notification procedures includes the notification mechanism, notification period for comments, mechanism to receive, review and incorporate the comments, mechanism for final changes to the policy, and the period before final changes become effective.

* A list of specification components, subcomponents, and/or elements, changes to which require a change in certificate policy Object Identifier or CPS pointer (URL)..

4.8.2 Publication and Notification Procedures

This subcomponent contains the following elements:

* A list of components, subcomponents, and elements thereof that exist but that are not made publicly available; (33)

* Descriptions of mechanisms used to distribute the certificate policy definition or CPS, including access controls on such distribution.

4.8.3 CPS Approval Procedures

In a certificate policy definition, this subcomponent describes how the compliance of a specific CPS with the certificate policy can be determined.

5. OUTLINE OF A SET OF PROVISIONS

This section contains a possible outline for a set of provisions, intended to serve as a checklist or (with some further development) a standard template for use by certificate policy or CPS writers. Such a common outline will facilitate:

(a) Comparison of two certificate policies during cross-certification (for the purpose of equivalency mapping).

(b) Comparison of a CPS with a certificate policy definition to ensure that the CPS faithfully implements the policy.

(c) Comparison of two CPSs.

1. INTRODUCTION

1.1 Overview

1.2 Identification

1.3 Community and Applicability
- 1.3.1 Certification authorities
- 1.3.2 Registration authorities
- 1.3.3 End entities
- 1.3.4 Applicability

1.4 Contact Details
- 1.4.1 Specification administration organization

8.2 Publication and notification policies

8.3 CPS approval procedures

6. ACKNOWLEDGMENTS

The development of this document was supported by the Government of Canada's Policy Management Authority (PMA) Committee, the National Security Agency, the National Institute of Standards and Technology (NIST), and the American Bar Association Information Security Committee Accreditation Technical Working Group. Special thanks are due to Dave Fillingham, Jim Brandt, and Edmond Van Hees for their inspiration, support, and valuable inputs.

The following individuals also deserve credit for their review and input:

Teresa Acevedo, A&N Associates;
Michael Baum; VeriSign;
Sharon Boeyen, Entrust;
Bob Burger, McCarter & English;
Bill Burr, NIST;
Patrick Cain, BBN;
Michael Harrop, Government of Canada Treasury Board;
Rick Hornbeck, Digital Commerce Services;
Francois Marinier, Domus Software;
John Morris, CygnaCom Solutions;
Tim Moses, Entrust;
Noel Nazario, NIST;
John Nicolletos, A&N Associates;
Jean Petty, CygnaCom Solutions;
Denis Pinkas, Bull;
J.-F. Sauriol, Domus Software;
Robert Shirey, BBN;
Mark Silvern, VeriSign;
David Simonetti, Booz, Allen and Hamilton; and
Darryl Stal, Entrust.

Johnny Hsiung, and Chris Miller assisted in the preparation of the manuscript.

7. REFERENCES

[ABA1] American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, 1995.

[BAU1] Michael. S. Baum, Federal Certification Authority Liability

and Policy, NIST-GCR- 94-654, June 1994.

[ISO1] ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework," 1997 edition. (Pending publication of 1997 edition, use 1993 edition with the following amendment applied: Final Text of Draft Amendment DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, June 1996.)

[PEM1] S. Kent, "Privacy Enhancement for Internet Electronic Mail, Part II: Certificate-Based Key Management," Internet RFC 1422, 1993.

[PKI1] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure, Certificate and CRL Profile," RFC [tbd], 1998.

8. AUTHORS' ADDRESSES

Santosh Chokhani
CygnaCom Solutions, Inc.
Suite 100 West
7927 Jones Branch Drive
McLean, VA 22102

Phone: (703) 848-0883
Fax: (703) 848-0960
EMail: chokhani@cygnacom.com

Warwick Ford
VeriSign, Inc.
301 Edgewater Place, Suite 210
Wakefield, MA 01880

Phone: (781) 245-6996 x225
Fax: (781) 245-6006
EMail: wford@verisign.com

NOTES

1 The ABA Digital Signature Guidelines can be purchased from the ABA. See http://www.abanet.com for ordering details.

2 Examples of types of entity for subject CAs are a subordinate organization (e.g., branch or division), a federal government agency, or a state or provincial government department.

3 This statement can have significant implications. For example, suppose a bank claims that it issues CA certificates to its branches only. Now, the user of a CA certificate issued by the bank can assume that the subject CA in the certificate is a branch of the bank

4 Examples of the types of subject RA entities are branch and division of an organization.

5 Examples of types of subject end entities are bank customers, telephone company subscribers, and employees of a government department

6 This statement can have significant implications. For example, suppose Government CA claims that it issues certificates to Government employees only. Now, the user of a certificate issued by the Government CA can assume that the subject of the certificate is a Government employee.

7 Examples include X.500 distinguished name, Internet e-mail address, and URL.

8 The term "meaningful" means that the name form has commonly understood semantics to determine identity of the person and/or organization. Directory names and RFC 822 names may be more or less meaningful.

9 Examples of proof include the issuing CA generating the key, or requiring the subject to send an electronically signed request or to sign a challenge.

10 Examples of organization identity authentication are: articles of incorporation, duly signed corporate resolutions, company seal, and notarized documents.

11 Examples of individual identity authentication are: biometrics (thumb print, ten finger print, face, palm, and retina scan), driver's license, passport, credit card, company badge, and government badge.

12 Examples include duly signed authorization papers or corporate ID badge.

13 The identification policy for routine rekey should be the same as the one for initial registration since the same subject needs rekeying. The rekey authentication may be accomplished using the techniques for initial I&A or using digitally signed requests.

14 This identification and authentication policy could be the same as

that for initial registration.

15 This policy could be the same as the one for initial registration.

16 The identification policy for Revocation request could be the same as that for initial registration since the same subject certificate needs to be revoked. The authentication policy could accept a Revocation request digitally signed by subject. The authentication information used during initial registration could be acceptable for Revocation request. Other less stringent authentication policy could be defined.

17 The identification policy for key compromise notification could be the same as the one for initial registration since the same subject certificate needs to be revoked. The authentication policy could accept a Revocation request digitally signed by subject. The authentication information used during initial registration could be acceptable for key compromise notification. Other less stringent authentication policy could be defined.

18 The n out of m rule allows a key to be split in m parts. The m parts may be given to m different individuals. Any n parts out of the m parts may be used to fully reconstitute the key, but having any n- 1 parts provides one with no information about the key.

19 A key may be escrowed, backed up or archived. Each of these functions have different purpose. Thus, a key may go through any subset of these functions depending on the requirements. The purpose of escrow is to allow a third party (such as an organization or government) to legally obtain the key without the cooperation of the subject. The purpose of back up is to allow the subject to reconstitute the key in case of the destruction of the key. The purpose of archive is to provide for reuse of the key in future, e.g., use the private key to decrypt a document.

20 An example of activation data is a PIN or passphrase.

21 Examples of physical access controls are: monitored facility , guarded facility, locked facility, access controlled using tokens, access controlled using biometrics, and access controlled through an access list.

22 Examples of the roles include system administrator, system security officer, and system auditor. The duties of the system administrator are to configure, generate, boot, and operate the system. The duties of the system security officer are to assign accounts and privileges. The duties of the system auditor are to set up system audit profile, perform audit file management, and audit

review.

23 The background checks may include clearance level (e.g., none, sensitive, confidential, secret, top secret, etc.) and the clearance granting authority name. In lieu of or in addition to a defined clearance, the background checks may include types of background information (e.g., name, place of birth, date of birth, home address, previous residences, previous employment, and any other information that may help determine trustworthiness). The description should also include which information was verified and how.

24 For example, the certificate policy may impose personnel security requirements on the network system administrator responsible for a CA's network access.

25 Regardless of whether authorized persons are employees, practices should be implemented to ensure that each authorized person is held accountable for his/her actions.

26 A cryptographic module is hardware, software, or firmware or any combination of them.

27 The compliance description should be specific and detailed. For example, for each FIPS 140-1 requirement, describe the level and whether the level has been certified by an accredited laboratory.

28 Example of audit events are: request to create a certificate, request to revoke a certificate, key compromise notification, creation of a certificate, revocation of a certificate, issuance of a certificate, issuance of a CRL, issuance of key compromise CRL, establishment of trusted roles on the CA, actions of truste personnel, changes to CA keys, etc.

29 Example of archive events are: request to create a certificate, request to revoke a certificate, key compromise notification, creation of a certificate, revocation of a certificate, issuance of a certificate, issuance of a CRL, issuance of key compromise CRL, and changes to CA keys.

30 A parent CA is an example of audit relationship.

31 Example of compliance audit topics: sample check on the various I&A policies, comprehensive checks on key management policies, comprehensive checks on system security controls, comprehensive checks on operations policy, and comprehensive checks on certificate profiles.

32 The examples include, temporary suspension of operations until

deficiencies are corrected, revocation of entity certificate, change in personnel, invocation of liability policy, more frequent compliance audit, etc.

33 An organization may choose not to make public some of its security controls, clearance procedures, or some others elements due to their sensitivity.

34 All or some of the following items may be different for the various types of entities, i.e., CA, RA, and end entities.

LIST OF ACRONYMS

ABA - American Bar Association
CA - Certification Authority
CPS - Certification Practice Statement
CRL - Certificate Revocation List
DAM - Draft Amendment
FIPS - Federal Information Processing Standard
I&A - Identification and Authentication
IEC - International Electrotechnical Commission
IETF - Internet Engineering Task Force
IP - Internet Protocol
ISO - International Organization for Standardization
ITU - International Telecommunications Union
NIST - National Institute of Standards and Technology
OID - Object Identifier
PIN - Personal Identification Number
PKI - Public Key Infrastructure
PKIX - Public Key Infrastructure (X.509) (IETF Working Group)
RA - Registration Authority
RFC - Request For Comment
URL - Uniform Resource Locator
US - United States